



AF  
Zhd

PATENT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicant: **Siani Lynne Pearson, et al.** ) Examiner: Jeremiah L. AVERY  
)  
Serial No.: **10/049,213** ) Art Unit: 2131  
)  
Filed: February 5, 2002 ) Our Ref: B-4488 PCT 619500-7  
) 30990141-5 US  
)  
For: "ENFORCING RESTRICTIONS ON ) Date: September 25, 2006  
THE USE OF STORED DATA" )  
)  
) Re: ***Appeal to the Board of Appeals***

**BRIEF ON APPEAL**

Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

This is an appeal from the rejection dated April 26, 2006, for the above identified patent application. Appellants submit that this Appeal Brief is being timely filed because the Notice of Appeal was filed on July 25, 2006. Please deduct the amount of \$500.00 for the fee set forth in 37 C.F.R. 1.17(c) for submitting this Brief from deposit account no. 08-2025.

**REAL PARTY IN INTEREST**

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

09/27/2006 10:00:00 AM  
01-FC:1402  
500.00 PA  
082025 10049213

### **RELATED APPEALS AND INTERFERENCES**

There are no other appeals or interferences related to the present application.

### **STATUS OF CLAIMS**

Claims 1-44 are the subject of this Appeal and are reproduced in the accompanying appendix.

### **STATUS OF AMENDMENTS**

No Amendment After Final Rejection has been entered.

### **SUMMARY OF CLAIMED SUBJECT MATTER**

The invention claimed in claim 1 is directed to a computer system adapted to restrict operations on data, comprising a computer platform (10) having a secure operator (33) for checking whether a user of the platform is licensed to perform a requested operation on the data and for enabling use of the data; a portable trusted module (19) containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorized external modification; and an access profile (621) specifying license permissions of users with respect to the data; wherein the secure operator is adapted to check the access profile to determine whether a requested operation is licensed for the user identity contained in the portable trusted module and prevent the requested operation if a license is required and not present (*e.g.* p. 10. l. 24 – p. 22 l. 3, Figs. 1-7).

The invention claimed in claim 18 is directed to a computer system adapted to restrict operations on data, comprising a computer platform (10) having an access controller (30) for specifying license permissions of users with respect to the data and for enabling use of the data; a portable trusted module (19) containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorized external modification; wherein the access controller is adapted to determine whether a requested operation is licensed for the user identity contained in the portable trusted module and prevent the requested operation if a license is required and not present (*e.g.* p. 10. l. 24 – p. 22 l. 3, Figs. 1-7).

The invention claimed in claim 20 is directed to a method of restricting operations on data in a system comprising a computer platform (10) having a secure operator (33) for checking whether a user of the platform is licensed to perform a requested operation on the data and for enabling use of the data; a portable trusted module (19) containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorised external modification; and an access profile (621) specifying license permissions of users with respect to the data; the method comprising a request for a policy check by the operating system of the computer platform to the secure operator before acting upon the data, by sending to the secure operator the name of the target data plus the intended operation; the secure operator checking the restrictions associated with the target data in the access profile to determine whether the data may be operated upon; and the secure operator checking the proposed usage with the restrictions, and replying to the operating system (*e.g.* p. 10. l. 24 – p. 22 l. 3, p. 30 l. 25 – p. 37 l. 14, Figs. 1-7 & 20-22).

The invention claimed in claim 26 is directed to a method of installing data on to a computer platform for restricted use thereon, the computer platform comprising a computer platform (10) having a secure operator (33) for checking whether a user of the platform is licensed to perform a requested operation on the data and for enabling use of the data, a platform trusted module (24) wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorised external modification, and a data protector (1207) for checking data integrity before a processor of the computer platform carries out operations on the data; the method comprising verification of the reliability of the data before installation of the data and an associated access profile and loading of a digest of protected data and an associated access profile into the platform trusted module, whereby the digest is used by the data protector and/or secure operator before execution of the data (*e.g.* p. 10. l. 24 – p. 22 l. 3, p. 27 l. 23 – p. 28 l. 8, p. 30 l. 25 – p. 37 l. 14, Figs. 1-7, 16 & 20-22).

The invention claimed in claim 27 is directed to a computer platform (10) having a secure operator (33) for checking whether a user of the platform is licensed to perform a requested operation on the data and for enabling use of the data and access profile (621) specifying license permissions of users with respect to the data; wherein the secure operator is adapted to check the access profile to determine whether a requested operation is licensed for a user identity contained

in a portable trusted module (19) in communication with the computer platform, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorised external modification, and prevent the requested operation if a license is required and not present (*e.g.* p. 10. l. 24 – p. 22 l. 3, Figs. 1-7).

The invention claimed in claim 39 is directed to a portable trusted module (19) containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorised external modification; the portable trusted module containing a user access license specifying access rights to data associated with the portable trusted module (*e.g.* p. 10. l. 24 – p. 22 l. 3, Figs. 1-7).

The invention claimed in claim 41 is directed to a method of restricting operations on data in a system comprising a computer platform (10) having an access controller (30) specifying license permissions of users with respect to the data; and for enabling use of the data; a portable trusted module (19) containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorised external modification; the method comprising a request for a policy check by the operating system of the computer platform to the access controller before acting upon the data, by sending to the access controller the name of the target data plus the intended operation; the access controller checking the restrictions associated with the target data to determine whether the data may be operated upon; and replying to the operating system (*e.g.* p. 10. l. 24 – p. 22 l. 3, p. 30 l. 25 – p. 37 l. 14, Figs. 1-7 & 20-22).

### **GROUND OF REJECTION TO BE REVIEWED ON APPEAL**

Issue 1: Whether the drawings presented with the preliminary amendment of February 5, 2002 are acceptable.

Issue 2: Whether claims 1-15, 18-22, 24, and 26-44 are patentable under 35 USC 102(e) in view of U.S. Patent 5,943,423 to Muftic (hereinafter “Muftic”).

Issue 3: Whether claims 16 and 25 are patentable under 35 U.S.C. 103(a) over Muftic as applied to claims 2 and 21 above (respectively) and further in view of U.S. Patent 6,091,835 to Smithies, et al. (hereinafter “Smithies, et al.”).

Issue 4: Whether claim 23 is patentable under 35 U.S.C. 103(a) over Muftic as applied to claim 21 and further in view of U.S. Patent 5,870,723 to Pare (hereinafter "Pare").

### **GROUPING OF CLAIMS**

For each ground of rejection which Appellants contest herein and which applies to more than one claim, such additional claims, to the extent separately identified and argued below, do not stand or fall together.

### **ARGUMENT**

**Issue 1: Whether the drawings presented with the preliminary amendment of February 5, 2002 are acceptable.**

In the second section identified as section 1 of the Office Action of April 26, the Examiner continues to object to the drawings because of the "mislabeling of Figure 21," explaining that "among the drawing sheets there is a figure labeled 'Fig. 22' which matches the description of Figure 21." Specifically, the Examiner complains that the drawings submitted via preliminary amendment on February 5, 2002 did not each contain a label stating "Annotated Sheets". Appellants respectfully direct the Board's attention to page 1 of the amendment which clearly requests the Examiner to "approve the amendments to the drawings, indicated in red." There were no replacement sheets submitted, but rather proposed drawing amendments which the Examiner to this date has yet to specifically approve, preferring instead to delay prosecution by raising form over substance and insisting on labels on the proposed amended drawings. Appellants respectfully request the Board of Appeals to forgive the omission of labels, which would be redundant given that only annotated sheets were submitted, and to concentrate instead on the substance of the proposed amendments (as the Examiner has so far failed to do) and expressly approve the amendments. Once approved, Appellants will provide formal amended replacement figures, all with appropriate labels of course.

**Issue 2: Whether claims 1-15, 18-22, 24, and 26-44 are patentable under 35 USC 102(e) in view of U.S. Patent 5,943,423 to Muftic (hereinafter “Muftic”).**

In section 3 the Examiner rejects claims 1-15, 18-22, 24, and 26-44 under 35 USC 102(e) as being anticipated by U.S. Patent 5,943,423 to Muftic. In particular, with regards to claims 1, 18 and 27, the Examiner finds that Muftic discloses all claimed limitations. In their last submission, Appellants endeavored to explain to the Examiner why this is not correct. Muftic does not in fact disclose a number of the claimed limitations, including at the very least a portable trusted module and an access profile. The Examiner notes that “[p]erforming ‘cryptographic functions and transformations’ assists in protecting the contents found in the trusted module (‘smart token’).” However, Muftic discloses the use of smart cards “programmed to perform cryptographic functions and transformations based on at least one cryptographic algorithm,” col. 3, lines 40-42, and “generating transactions [with the use of a smart card and a smart card reader] which are at least partially encrypted and/or digitally signed,” col. 4, lines 1-2, and which is certainly not a disclosure of a trusted module that is a “component adapted to behave in an expected manner and resistant to unauthorized external modification” as presently claimed. As for the Examiner’s allegation that Muftic teaches “an access profile specifying license permissions of users with respect to the data” at col. 5, lines 48-54, Appellants had explained that the cited section of Muftic teaches only that activities in a computing environment are authorized “only to those persons authorized to engage in the activity by opening an authorization credentials application domain on a smart token; scanning a plurality of authorization credentials stored therein for an authorizing credential; and if an authorizing credential is found, authorizing the activity.” Thus, it is clear that Muftic teaches the binding of a key pair to license-related software and to a particular user identity (*see, e.g.*, col. 5 l. 55 - col. 6 l. 4). This is not “an access profile specifying license permissions of *users*” or “an access controller for specifying license permissions of *users*.” In Muftic the software is bound specifically to one user identity and cannot be used by others, whereas in the claimed invention the secure operator is adapted to check the access profile to determine whether a requested operation is licensed for the user identity contained in the portable trusted module and prevent the requested operation if a license is required and not present (as per claim 1).

Presently the Examiner attempts to create the illusion of a reply by asserting that “the disclosure of smart cards and PCMCIA cards, *as broadly interpreted* by the Examiner, by Muftic discloses said ‘portable trusted module.’ Also, the ‘cryptographic functions’ as disclosed by Muftic *could be* utilized in the prevention of ‘unauthorized external modification.’” To this Appellants can only but reply, huh? The lack of support for either of these assertions on the face of Muftic itself is so utter as to border on the desolate. The Examiner’s interpretation is in fact so broad as to encompass a whole slew of ideas that are not to be found anywhere in Muftic – only to be found, in fact, in Appellants’ claims. The leap from the rather cursory mention of smart cards and PCMCIA cards in Muftic to the “portable trusted module” as per Appellants’ claims is of breathtaking scope and enviable ambition but completely lacking in the slightest of hints from Muftic himself, as can be quickly inferred from the Examiner’s lack of offering beyond his “broad interpretation.”

The Examiner’s “explanation” of where Muftic discloses the claimed access profile is almost giggle-inducing. Maybe something in Muftic *could* indeed be used by one skilled in the art, in some manner, in the practice of Appellants’ invention – but how does this anticipate the claim limitation in question? Where does Muftic specifically state that the cryptographic functions as disclosed could be utilized in the prevention of unauthorized external modification? And where does Muftic specifically teach how the skilled person would go about utilizing the cryptographic functions as disclosed in the prevention of unauthorized external modification?

The Examiner’s imagination only seems to take flight with his ensuing “replies.”

With regards to Appellants’ argument that Muftic also does not disclose an access profile specifying license permissions of users with respect to the data as per claim 20, the Examiner once again flexes his broad interpretation muscles and offers that “the ‘authorization credentials as disclosed by Muftic are broadly interpreted by the Examiner as pertaining to, inter alia, ‘license permission’” because “a license can be a certification of authority which would allow a specific user(s) to be able to engage in designated activities, as granted by said authority.” The Examiner does not bother to make the connection between his broad interpretation of what a license can be, what Muftic actually discloses, and the claimed *access profile* specifying license permissions of users with respect to the data, but he does offer this gem: “[f]urthermore, an ‘access profile’ exists within the teachings of Muftic for in order to determine whether or not a

user can obtain access, a set of credentials and identification means are stored and associated with each user, thus providing the creation of a form of an ‘access profile’ which will either allow or restrict access, dependent upon, inter alia, said credentials.” At the risk of sounding like a broken record, Appellants once again beg – **where** does Muftic disclose this? **Where** is it stated, hinted, or alluded to, that a set of credentials and identification means are stored and associated with each user? And what does **a form** of access profile as imagined by the Examiner have to do with Appellants claimed access profile and it’s very clearly delineated bounds? **Why** does the Examiner so completely flaunt the clear requirements of M.P.E.P. § 2131?

As for claim 41, Appellants had previously enumerated all the claimed limitations missing from Muftic, and which the Examiner now once again conveniently imagines to find in Muftic. Specifically, and puzzlingly, the Examiner now asserts that “the ‘activation and access test’ as disclosed by Muftic can be utilized for ‘access control purposes’ *which pertains to the embodiment as claimed in the present invention*” but cunningly hides from us exactly **how** this can be done, and grandly concludes with “[f]urthermore, the ‘interrogation/response mode’ *can be used for*, inter alia, policy checking.” Wearily, Appellants yet again ask – how? And even if true, so what? The Examiner is rejecting the claims under 35 U.S.C. §**102**. The Examiner’s bald and unsupported assertions, given the very utmost benefit of a doubt, would still require at the very least combining with some knowledge commonly within the ambit of those of ordinary skill in the art – something the Examiner could learn a lot about in MPEP §706.02(j) and on, which discusses rejections under 35 U.S.C. §**103 - OBVIOUSNESS**.

The Examiner’s “answers” to Appellants’ arguments regarding the other claims are basically a repetition of what has already been addressed above. Appellants thus wish to simply conclude by respectfully submitting to the Board that the Examiner’s continued rejection of the claims in view of the Muftic reference is unsupported and unsupportable because it severely mischaracterizes the teachings of this reference and seeks to fill in expansive gaps in its teachings with bald assertions of purposes for which what the reference does actually disclose allegedly *could be* used for – and which thereby on its very face proves that the Examiner implicitly agrees that Muftic does not disclose each and every claimed limitation. Appellants thus respectfully request the Board to overturn the Examiner on appeal and pass all independent



claims to issue in view of the above discussion, and to further pass all dependent claims to issue based at least upon their respective dependencies on allowable independent claims.

**Issue 3: Whether claims 16 and 25 are patentable under 35 U.S.C. 103(a) over Muftic as applied to claims 2 and 21 (respectively) and further in view of U.S. Patent 6,091,835 to Smithies, et al. (hereinafter “Smithies”).**

In section 28 the Examiner rejects claims 16 and 25 under 35 USC 103(a) as being unpatentable over Muftic as applied to claims 2 and 21 above (respectively) and further in view of U.S. Patent 6,091,835 to Smithies. In section 33 the Examiner further rejects claims 17 in view of Muftic and Smithies. Appellants traverse the Examiner’s rejections but do not address them on the merits because claims 16, 17 and 25 depend from independent claims that have been shown above to be allowable, and thus claims 16, 17 and 25 are also allowable at least based on their dependencies.

**Issue 5: Whether claim 27 is patentable under 35 U.S.C. 101 over claim 27 of co-pending application S/N 10/049,211 (the “‘211 application”).**

In section 43 the Examiner continues to provisionally reject claim 27 under 35 USC 101 as claiming the same invention as that of claim 27 of co-pending application No. 10/049,211. In their previous submission Appellants explained that this rejection should be withdrawn because the identical subject matter is not defined by both claims. Specifically, claim 1 of the ‘211 application (from which claim 27 indirectly depends) contains, *inter alia*, the following limitation: “[a] computer platform having: a trusted module which is resistant to internal tampering and which stores a third party’s public key certificate.” This limitation comes before the “a further, removable, trusted module containing a user identity” added by claim 27 of the ‘211 application. Claim 27 of the present application does not contain this limitation. It does contain a limitation directed to “a portable trusted module in communication with the computer platform, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorised external modification,” but the “portable trusted module” of claim 27 of the instant application is not a part of the computer platform and therefore is not substantively the same as the “trusted module” in the computer platform of claim 27 of the ‘211 application.

Thus, even without considering the other limitations, a computer platform lacking a "trusted module" or its equivalent in its computer platform that could infringe claim 27 of the instant '213 application could not infringe claim 27 of the '211 application.

In his current "answer" the Examiner resorts to arguing semantics and, blithely ignoring all of the above, asserts that "usage of synonymous terms does not differentiate each application for patentability." The Examiner thus clearly ignores the limitations regarding the presently claimed portable trusted module, choosing instead to rely on the recitation in claim 27 of the '211 application of the *similarly-sounding* removable, trusted module. Appellants thus respectfully request the Board to accord the full attention and consideration to the above argument that the Examiner could not be bothered to, and to withdraw this double patenting rejection for being based upon an improper reading of the claims of the two applications.

In view of all the above, Appellants respectfully submit that all pending claims are novel and nonobvious and request the Board to overturn the Examiner's rejection of the claims on appeal and pass the case to allowance.

### CONCLUSION

For the many reasons advanced above, Appellants respectfully contend that each claim is patentable and reversal of all rejections and allowance of the case is respectfully solicited.

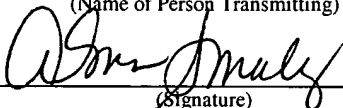
I hereby certify that this correspondence is being deposited with the United States Post Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

September 25, 2006

(Date of Transmission)

Alma Smalling

(Name of Person Transmitting)



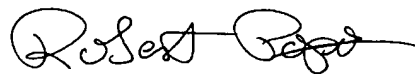
(Signature)

9/25/06

(Date)

Attachments

Respectfully submitted,



Robert Popa

Attorney for Appellants

Reg. No. 43,010

LADAS & PARRY

5670 Wilshire Boulevard, Suite 2100

Los Angeles, California 90036

(323) 934-2300 voice

(323) 934-0202 facsimile

rpopa@ladasperry.com

Claims

---

1. A computer system adapted to restrict operations on data, comprising:

a computer platform having a secure operator for checking whether a user of the platform is licensed to perform a requested operation on the data and for enabling use of the data;

a portable trusted module containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorized external modification;

and an access profile specifying license permissions of users with respect to the data;

wherein the secure operator is adapted to check the access profile to determine whether a requested operation is licensed for the user identity contained in the portable trusted module and prevent the requested operation if a license is required and not present.

2. A computer system as claimed in claim 1, wherein the computer platform further comprises a platform trusted module, and wherein the platform trusted module and the portable trusted module are adapted for mutual authentication.

3. A computer system as claimed in claim 2, wherein some or all of the functionality of the secure operator is within the platform trusted module.

4. A computer system as claimed in claim 1, wherein the access profile is within the computer platform.

5. A computer system as claimed in claim 1, wherein some or all of the data is within the computer platform, and the computer platform further comprises a data protector for checking data integrity before a processor of the computer platform carries out operations on the data.

6. A computer system as claimed in claim 1, wherein some or all of the data is within the portable trusted module or in a device containing the portable trusted module, and the portable trusted module or the device containing the portable trusted module further comprises a data protector for checking data integrity before a processor of the computer platform carries out operations on the data.

7. A computer system as claimed in claim 5, wherein the data protector is within the relevant trusted module.

8. A computer system as claimed in claim 5, wherein the data protector is adapted to check installation of data and to load a digest of protected data and/or any associated access profile into the relevant trusted component.

9. A computer system as claimed in claim 1, wherein the trusted platform is adapted at boot to check the integrity of operation protection code comprising the secure operator and, if present, the data protector.

10. A computer system as claimed in claim 9, wherein the computer platform further comprises a platform trusted module,

and wherein the platform trusted module and the portable trusted module are adapted for mutual authentication, and wherein the computer platform is adapted to perform the integrity check by reading and hashing the operation protection code to produce a first hash, reading and decrypting a stored signed version of a secure operation protection code hash using a public key certificate of a third party stored in the platform trusted module to produce a second hash, and comparing the first hash and the second hash.

11. A computer system as claimed in claim 1, wherein the portable trusted module contains a user access license specifying access rights to the data associated with the removable trusted module, whereby unless prevented by the access profile, the secure operator is adapted to check the user access license to determine whether a requested operation is licensed for the user identity contained in the portable trusted module.

12. A computer system as claimed in claim 2, wherein the computer platform comprises a secure communication path between the platform trusted module and the operating system of the computer platform.

13. A computer system as claimed in claim 1, wherein the computer platform is adapted such that:

the operating system requests a policy check from the secure operator before acting upon the data, by sending the name of the target data plus the intended operation;

the secure operator checks the restrictions associated with the target data in the access profile, to determine whether the data may be operated upon; and

the secure operator checks the proposed usage with the restrictions, and replies to the operating system.

14. A computer system as claimed in claim 13, wherein the computer platform further comprises a platform trusted module, wherein the platform trusted module and the portable trusted module are adapted for mutual authentication, and wherein some or all of the functionality of the secure operator is within the platform trusted module; wherein on request by the operating system for permission to operate on the data, the secure operator sends a message to the access profile signed with a private key of the platform trusted module, wherein the access profile has access to the public key of the platform trusted module and can verify and authenticate the signed message with said public key, whereby if satisfied the access profile sends access profile data to the secure operator, whereupon the secure operator tests the access profile data and if appropriate requests the operating system to carry out the operation requested.

15. A computer system as claimed in claim 13, wherein the computer platform further comprises a platform trusted module, and wherein the platform trusted module and the portable trusted module are adapted for mutual authentication, and wherein the computer system further comprises a data protector for checking data integrity before a processor of the computer platform carries out operations on the data; wherein the relevant trusted component contains a secure result of a one-way function on the data and associated access profile, and the data protector prevents the operation from being carried out if calculation of

the one-way function provides a result different from the secure result.

16. A computer system as claimed in claim 2, wherein the platform trusted component is adapted to log requests to the operating system to perform particular operations on the data.

17. A computer system as claimed in claim 6, wherein the portable trusted component is adapted to log requests to the operating system to perform particular operations on the data.

18. A computer system adapted to restrict operations on data, comprising:

a computer platform having an access controller for specifying license permissions of users with respect to the data and for enabling use of the data;

a portable trusted module containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorized external modification;

wherein the access controller is adapted to determine whether a requested operation is licensed for the user identity contained in the portable trusted module and prevent the requested operation if a license is required and not present.

19. A computer system as claimed in claim 18, wherein the operating system of the computer platform is adapted to request a policy check from the access controller before carrying out certain operations on the data, whereupon the access controller checks restrictions applying to the data to determine whether

the data may be operated on, and replies to the operating system accordingly.

20. A method of restricting operations on data in a system comprising:

computer platform having a secure operator for checking whether a user of the platform is licensed to perform a requested operation on the data and for enabling use of the data;

a portable trusted module containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorised external modification;

and an access profile specifying license permissions of users with respect to the data;

the method comprising a request for a policy check by the operating system of the computer platform to the secure operator before acting upon the data, by sending to the secure operator the name of the target data plus the intended operation;

the secure operator checking the restrictions associated with the target data in the access profile to determine whether the data may be operated upon; and

the secure operator checking the proposed usage with the restrictions, and replying to the operating system.

21. A method as claimed in claim 20, wherein the computer platform further comprises a platform trusted module, and wherein some or all of the functionality of the secure operator is within the platform trusted module, and whereby on request by the operating system for permission to operate on the data, the secure operator sends a message to the access profile signed



with a private key of the platform trusted module, wherein the access profile has access to the public key of the platform trusted module and can verify and authenticate the signed message with said public key, whereby if satisfied the access profile sends access profile data to the secure operator, whereupon the secure operator tests the access profile data and if appropriate requests the operating system to carry out the operation requested.

22. A method as claimed in claim 21, wherein the computer platform further comprises a data protector for checking data integrity before a processor of the computer platform carries out operation on the data, and wherein the platform trusted component contains a secure result of a one-way function on the data and associated access profile, and the data protector prevents the operation from being carried out if calculation of the one-way function provides a result different from the secure result.

23. A method as claimed in claim 21, wherein before execution of the data, the data protector checks that there are not multiple copies of the data stored within the computer platform and prevents data execution if there are multiple copies.

24. A method as claimed in claim 21, wherein the computer platform comprises a secure communication path between the platform trusted component and the operating system, and whereby the request from the secure operator to the operating system to use the data is provided on the secure communication path.

25. A method as claimed in claim 21, wherein the platform trusted module is adapted to log any request to the operating system to perform a particular operation on the data.

26. A method of installing data on to a computer platform for restricted use thereon, the computer platform comprising:  
a computer platform having a secure operator for checking whether a user of the platform is licensed to perform a requested operation on the data and for enabling use of the data, a platform trusted module wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorised external modification, and a data protector for checking data integrity before a processor of the computer platform carries out operations on the data;  
the method comprising verification of the reliability of the data before installation of the data and an associated access profile and loading of a digest of protected data and an associated access profile into the platform trusted module, whereby the digest is used by the data protector and/or secure operator before execution of the data.

27. A computer platform having a secure operator for checking whether a user of the platform is licensed to perform a requested operation on the data and for enabling use of the data and access profile specifying license permissions of users with respect to the data; wherein the secure operator is adapted to check the access profile to determine whether a requested operation is licensed for a user identity contained in a portable trusted module in communication with the computer platform, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorised

external modification, and prevent the requested operation if a license is required and not present.

28. A computer platform as claimed in claim 27, further comprising a platform trusted module, and wherein the platform trusted module and the portable trusted module are adapted for mutual authentication.

29. A computer platform as claimed in claim 28, wherein some or all of the functionality of the secure operator is within the platform trusted module.

30. A computer platform as claimed in claim 27, wherein the access profile is within the platform trusted module.

31. A computer platform as claimed in claim 27, wherein some or all of the data is within the computer platform, and the computer platform further comprises a data protector for checking data integrity before a processor of the computer platform carries out operations on the data.

32. A computer platform as claimed in claim 31, wherein the data protector is within the platform trusted module.

33. A computer platform as claimed in claim 31, wherein the data protector is adapted to check installation of data and to load a digest of protected data and/or any associated access profile into the platform trusted component.

34. A computer platform as claimed in claim 27, wherein the computer platform is adapted at boot to check the integrity of

operation protection code comprising the secure operator and, if present, the data protector.

35. A computer platform as claimed in claim 28, further comprising a secure communication path between the platform trusted module and the operating system of the computer platform.

36. A computer platform as claimed in claim 27, adapted such that:

the operating system requests a policy check from the secure operator before acting upon the data, by sending the name of the data plus the intended operation;

the secure operator checks the restrictions associated with the target data in the access profile, to determine whether the data may be operated upon; and

the secure operator checks the proposed usage with the restrictions, and replies to the operating system.

37. A computer platform as claimed in claim 36, further comprising a platform trusted module, and wherein the platform trusted module and the portable trusted module are adapted for mutual authentication, wherein on request by the operating system for permission to operate on the data, the secure operator sends a message to the access profile signed with a private key of the platform trusted module, wherein the access profile has access to the public key of the platform trusted module and can verify and authenticate the signed message with said public key, whereby if satisfied the access profile sends access profile data to the secure operator, whereupon the secure operator tests the access profile data and if appropriate

requests the operating system to carry out the operation requested.

38. A computer platform as claimed in claim 31, further comprising a platform trusted module, and wherein the platform trusted module and the portable trusted module are adapted for mutual authentication, wherein the platform trusted component contains a secure result of a one-way function on the data and associated access profile, and the data protector prevents the operation from being carried out if calculation of the one-way function provides a result different from the secure result.

39. A portable trusted module containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorised external modification; the portable trusted module containing a user access license specifying access rights to data associated with the portable trusted module.

40. A portable trusted module as claimed in claim 39 and located within a smart card.

41. A method of restricting operations on data in a system comprising:

- a computer platform having an access controller specifying license permissions of users with respect to the data; and for enabling use of the data;

- a portable trusted module containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorised external modification;

the method comprising a request for a policy check by the operating system of the computer platform to the access controller before acting upon the data, by sending to the access controller the name of the target data plus the intended operation;

the access controller checking the restrictions associated with the target data to determine whether the data may be operated upon; and

replying to the operating system.

42. A method as claimed in claim 41, wherein the computer platform further comprises a platform trusted module, and wherein some or all of the functionality of the access controller is within the platform trusted module.

43. A computer system as claimed in claim 6, wherein the data protector is within the relevant trusted module.

44. A computer system as claimed in claim 6, wherein the data protector is adapted to check installation of data and to load a digest of protected data and/or any associated access profile into the relevant trusted component.

There is no evidence submitted with the present Brief on Appeal.

U. S. Appln. No. 10/049,213

Brief on Appeal dated September 25, 2006

In support of Notice of Appeal submitted July 25, 2006

Related Proceedings Appendix Page C-1

---

There are no other appeals or interferences related to the present application.